FIVERS

Regulatory update
Data protection, AI, IT and IP

No. 3 / 2025

DATA PROTECTION.

5 February 2024 – Supreme Court of Cassation: order 807/2025 specifies that defensive checks on the worker's email cannot be retroactive to the onset of the suspicion of wrongdoing.

---

1 February 2025 – The French Data Protection Authority (CNIL) publishes a guide on how to carry out the Data Transfer Impact Assessment (DTIA).

---

31 January 2025 – The French Data Protection Authority (CNIL) has put out a European certification scheme for the external data processor for public consultation.

ARTIFICIAL INTELLIGENCE.

4 February 2025 – EU Commission: published the Guidelines on Artificial Intelligence practices prohibited under Regulation 2024/1689 (AI Act).

---

2 February 2024 – EU Regulation 2024/1689 on Artificial Intelligence: the first 5 articles are applicable.

---

23 January 2024 – European Data Protection Board: two reports released on (1) data governance against algorithmic discrimination and (2) effectiveness of the exercise of data protection rights in the AI context.

DIGITAL MARKETPLACES

2 February 2025 – Draft legislative decree coordinating Regulation 2022/2554 on Digital Operational Resilience (DORA) to national law.

INFORMATION TECHNOLOGY

28 January 2025 – Court of Cassation: even if the recipient of a PEC claims not to have received the notification, it is completed with the receipt of delivery.

---

24 January 2025 – Constitutional Court: the rules of the Digital Administration Code (CAD) that have the effect of preventing disabled people from using the digital signature to sign the electoral rolls are unconstitutional.

DATA PROTECTION

5 February 2024 – Supreme Court of Cassation: order 807/2025 specifies that defensive checks on the worker's email cannot be retroactive to the onset of the suspicion of wrongdoing.

The Court of Cassation, with order no. 807/2025, provided relevant indications regarding the defensive controls and the limits of such checks that employers can carry out on their employees' company emails in the event of a suspicion of wrongdoing.
The decision establishes that these checks cannot be retroactive, i.e. they cannot concern communications prior to the emergence of the well-founded suspicion of wrongdoing that enables defensive control.

The possibility for employers to monitor workers' e-mail communications for defensive control purposes has generated numerous legal discussions, leading the Supreme Court to define more precisely the limits within which such controls can take place.

With its recent order, the Supreme Court clarified that defensive checks by the company are legitimate only if conducted on data collected after the emergence of concrete suspicions.

One of the fundamental aspects sanctioned by the Supreme Court is the impossibility of examining the emails sent or received before the doubt arises about a possible irregularity. This limitation is necessary to ensure a balance between the protection of corporate interests and the right to privacy of workers, both of which are protected by current regulations.

---

1 February 2025 – The French Data Protection Authority (CNIL) publishes a guide on how to carry out the Data Transfer Impact Assessment (DTIA).

The French data protection authority, CNIL, has published a Data Transfer Impact Assessment (DTIA) guide to help organizations transfer personal data outside of the European Economic Area (EEA) in compliance with the GDPR.

The guidance outlines the process for the execution of a DTIA when using Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) and details when a DTIA is not required, for example for countries with an adequacy decision or exemptions under Article 49.

It provides a five-step roadmap for the execution of a DTIA and recommends six measures to ensure effective data transfer, including assessing third country laws, identifying risks, and implementing additional measures.

---

31 January 2025 – The French Data Protection Authority (CNIL) has put out a European certification scheme for the external data processor for public consultation.

The French data protection authority, CNIL, has launched a consultation for asystem for certifying data controllers under the GDPR, open to European organisations that process personal data on behalf of a data controller.

In particular, the CNIL highlighted that all European-based organizations that process personal data on behalf of a data controller will be able to apply for certification. Small and medium-sized enterprises are encouraged to apply. The obligations of data processors apply to all organizations that process data on behalf of a data controller and may include: IT service providers; software house ; IT security companies; digital service companies that have access to data; marketing or communication companies.

The certification is designed to be generalist, covering a wide range of data processing activities and comprising 90 five-part control points, from contracting to action plans during the three-year certification period. The public consultation will run until 28 February 2025.

ARTIFICIAL INTELLIGENCE.

4 February 2025 – EU Commission: Guidelines on prohibited Artificial Intelligence practices under Regulation 2024/1689 (AI Act) approved.

In conjunction with the direct applicability – as of 2 February 2025 – of Article 5 of Regulation 2024/1689 on AI, which prohibits the so-called "*prohibited artificial intelligence practices*", the EU Commission has approved (although not yet formally adopted) the Communication containing the Guidelines on prohibited AI practices pursuant to EU Regulation 2024/1689.

The guidelines specifically address – with operational and interpretative (non-binding) guidance on bans – practices such as malicious manipulation, social scoring, and real-time remote biometric identification, among others. They also provide legal clarifications and practical examples useful for understanding and complying with the requirements of the AI Act.

The setting of the guidelines is very concrete and useful: for each prohibited AI practice, the Commission provides an analysis of the regulatory logic, objectives of the ban, main conceptual and interpretative characteristics, type of behaviour that falls under the ban, legal behaviour or behaviour outside the ban, interconnection with other EU legislation (e.g. GDPR), cases of exclusion, practical examples.

---

2 February 2024 – EU Regulation 2024/1689 on Artificial Intelligence: the first 5 articles are applicable.

As of February 2, 2025, EU Regulation 2024/1689 on Artificial Intelligence begins to be applicable. The so-called AI Act came into force on August 1, 2024, but will be applicable at deferred deadlines, between 6 and 36 months from the date of entry into force. From 2 February 2025, Chapters I and II and the first 5 articles of the AI Act are fully applicable. From a practical point of view, for example, it is possible to make use (in supply contracts) of the 68 technical definitions set out in Article 3 (starting with the definition of "*artificial intelligence system*" and "*artificial intelligence model*"), while "AI literacy" becomes mandatory for suppliers, companies and users" i.e. the obligation (including training) to have sufficiently trained staff with basic skills in the use of AI. Finally, the prohibition of certain artificial intelligence practices, some of which relate to the use of AI in the workplace, is applicable.

---

24 January 2024 – European Data Protection Board: two reports released on (1) data governance against algorithmic discrimination and (2) effectiveness of the exercise of data protection rights in the context of AI.

The European Data Protection Board (EDPB) has published the two reports (1) "*AI-Complex Algorithms and effective Data Protection Supervision - Bias evaluation*" and (2) "*AI-Complex Algorithms and effective Data Protection Supervision - Effective implementation of data subjects' rights*".

The Algorithmic Discrimination Assessment (blas) report identifies various sources of bias in artificial intelligence, starting with incomplete or inaccurate data, and proposes mitigation measures both in the pre-treatment phase and in the subsequent post-processing phase in *machine learning*. It also acknowledges the current limitations of tools to detect and mitigate bias in generative AI systems.

In the second report on the implementation of data subject rights in the AI context, the analysis examines the challenges related to the implementation of data subject rights in AI, proposing methods for data deletion and *unlearning* or *differential privacy* to limit the influence of individual data points. Unlearning refers to the process of removing knowledge or information learned from a machine learning model or AI system. There are essentially two approaches: **(1)** *model-agnostic unlearning*, which does not depend on the specific architecture or operation of the model and is a generic method applicable to any system, regardless of the type of underlying model; and **(2)** *application-specific* unlearning, which instead is based on the

adaptation of the unlearning method to the model or specific case, exploiting the knowledge of the architecture and operation of the system.

Differential Privacy (DP) is a mathematical framework used to protect the privacy of individuals in a dataset by limiting the influence of individual data points on the outcome of an analysis or model. Essentially, a mechanism satisfies differential privacy if the addition or removal of a single piece of data in the dataset changes the outcome of the algorithm in a negligible way. This ensures that an individual's personal data cannot be identified or reconstructed, even when the model or result is published.

DIGITAL MARKETPLACES

2 February 2025 – Draft legislative decree coordinating Regulation 2022/2554 on Digital Operational Resilience (DORA) to national law.

The draft implementing decree coordinates the provisions of Regulation (EU) 2022/2554 (DORA) with national law and is divided into six chapters, defining, among other things, the competent authorities at national level and the role of the *Computer Security Incident Response Team* (CSIRT) Italy.

Pursuant to Article 46 of the DORA Regulation, supervisory responsibilities are divided among different Authorities, each of which exercises its functions according to specific powers. Especially:

- Bank of Italy: exercises supervisory powers over financial intermediaries, Bancoposta and Cassa Depositi e Prestiti S.p.A., ensuring compliance with the obligations set out in the DORA Regulation;

- Consob: participates as an observer in the surveillance forum;

- IVASS and COVIP: act as observers in relation to matters of their respective competence.

In application of the provisions of the DORA Regulation, the related delegated acts, the regulatory and implementing technical standards, as well as the implementing provisions of the draft decree, the competent authorities have specific supervisory powers. These powers include the power to take action against supervised financial entities; of Cassa Depositi e Prestiti S.p.A.; financial intermediaries and Bancoposta; third-party ICT (ICT) service providers that support *essential or important functions* for the financial sector.

The supervisory powers, enshrined in Articles 50(2) and 42(6) of the DORA Regulation, extend to those already provided for by the sectoral legislation and the draft implementing decree. In concrete terms, the Authorities can carry out inspections and audits at third-party ICT service providers; convene directors, members of the board of statutory auditors and staff of supervised entities; request information, documentation and clarifications regarding ICT risk management.
These powers are in addition to those already attributed by sectoral disciplines, including the Consolidated Banking Act (TUB), the Consolidated Law on Finance (TUF) and the Private Insurance Code (CAP). Furthermore, the provisions contained in Articles 51, 53-bis, 54 and 108 of the TUB, as well as other related rules, are included among the intervention instruments.

One of the most important aspects of the draft decree is represented by the sanctioning regime outlined in Article 10. The system provides for an articulation on several levels of responsibility, depending on the seriousness of the violation ascertained.

Financial penalties can be up to 10% of the annual turnover of the responsible financial entity, with differentiations based on the type of supervised entity:

- Banks, financial intermediaries and ICT service providers: fines ranging from a minimum of €30,000 to a maximum of 10% of turnover.
- Payment institutions and e-money institutions: penalties of up to €5 million or 10% of annual turnover, whichever is higher.
- Administrators, managers and staff with specific functions: for the most serious infringements, penalties of up to 5 million euros can be imposed.

In addition to financial penalties, the decree provides for ancillary measures, applicable in cases of particularly serious violations. These include:

- temporary disqualification from administrative, managerial or control positions for persons responsible for infringements;
- operational limitations for supervised entities, where necessary to protect the stability of the financial system.

The sanctioning system introduced by the draft decree is part of a broader regulatory framework, aimed at ensuring the effective implementation of the provisions of the DORA Regulation and strengthening the digital resilience of the financial sector.

INFORMATION TECHNOLOGY

28 January 2025 – Court of Cassation: even if the recipient of a PEC claims not to have received the notification, it is completed with the receipt of delivery.

The Court of Appeal had declared inadmissible, as it was belatedly filed, the appeal brought against the first instance judgment that had rejected a claim for damages. On the basis of its decision, the Court had considered the notification of the first instance judgment by certified email to the attorney constituted by the plaintiff to run as suitable for starting the short term to challenge pursuant to Article 326 of the Code of Civil Procedure.

The dispute reaches the Court of Cassation where the appellant criticizes the judgment under appeal for not having taken into account the legislation on the certainty of notifications to the parties, arguing in this sense that the answers received to the requests sent by the appellant's lawyer to the certified e-mail provider prove that he had never received anything.

The Supreme Court, however, specifies that the answers provided by the operator of telematic services to the request for clarification of the appellant's lawyer who claims to have received nothing do not count. In its arguments, the Court reiterates the recent principle according to which "*in the regime prior to the novelty brought by Legislative Decree no. no. 149 of 2022, service by certified email carried out by the lawyer pursuant to art. 3-bis of Law no. 53 of 1994 is not perfected in the event that the system generates a notice of non-delivery, even for reasons attributable to the addressee (as in the case of saturation of the PEC box with an error message with the wording "full box"), but only if the receipt of delivery (so-called "RfAC") is generated*".

In the present case – among other things – the Court noted that it was undisputed that such a receipt had been generated and produced among the documents filed by the applicant himself.

For this reason, the Supreme Court declared the appeal inadmissible.

---

23 January 2025 – Constitutional Court: the rules of the Digital Administration Code (CAD) that have the effect of preventing disabled people from using the digital signature to sign the electoral rolls are unconstitutional.

The Constitutional Court has declared the constitutional illegitimacy of art. 9, third paragraph, of Law 108 of 17 February 1968 and 2, paragraph 6, of the Digital Administration Code, in the part in which they do not provide for the voter who is unable to affix a handwritten signature due to certified impossibility deriving from a serious physical impediment or because he is in the condition to exercise home voting, the possibility of signing a list of candidates for the elections.

Technological development has made the tool inadequate, dating back to when the digital signature did not exist, which provided for the submitters of a list of candidates who were unable to sign due to physical

impediment, to be able to make their declaration in verbal form, in the presence of two witnesses, before a notary or the municipal secretary or other employee delegated for this purpose by the Mayor.

This procedure, in fact, presupposes "*that the persons authorized to receive the verbal statement and the witnesses go to the home of the person with a disability, with the consequence that the latter is required to take steps to obtain such presence, to bear any economic burdens, and, if necessary, to tolerate interference with his or her privacy*".

In these terms, the Constitutional Court concludes, "*the exclusion of the use of the digital signature also for people with disabilities determines the paradox that it is the legal system that, instead of removing the obstacles that prevent the full development of the human person and effective participation in the political organization, introduces itself "an increase that is neither necessary nor proportionate with respect to the need to verify the authenticity and genuineness of the signature of the list of candidates, which can also be achieved by allowing the voter with disabilities to use the electronic mode to support the list of candidates*"».
